JOURNAL OF ALGEBRA 77, 62–73 (1982)

On the Lüroth Semigroup and Weierstrass Canonical Divisors

T. T. MOH AND W. HEINZER*

Department of Mathematics, Purdue University, W. Lafayette, Indiana 47907

Communicated by I. N. Herstein

Received May 15, 1980

In [9] we generalized the classical Lüroth theorem to a statement concerning the degrees of irrationality of R and S, where $R \subseteq S$ are function fields of one variable over an infinite ground field. A more refined statement is Theorem 1 in the present article, which establishes a relationship between what we term the Lüroth semigroups of R and S, rather than just the degrees of irrationality. In Theorems 2 and 3 we generalize the classical result of Igusa [7] on Lüroth's theorem.

The concept of Weierstrass canonical divisors introduced here is clearly motivated by the classical concept of Weierstrass points. Using Weierstrass canonical divisors we obtain several results on Lüroth semigroups, and we give, in Theorem 4, a criterion for a field to be hyperelliptic.

To illustrate our results and the techniques involved, we give in Section 3 several examples and applications.

Our notation is, we hope, fairly standard. For example, for $x \in R$, a function field of one variable, we use (x) to denote the divisor of x, and $(x)_0$ and $(x)_\infty$ to denote, respectively, the zero divisor and polar divisor of x. If F and G are curves, we use $\#(F \cap G)$ to denote the number of intersections of F and G counted with multiplicities.

1. THE LÜROTH SEMIGROUP

DEFINITION—PROPOSITION 1. *Let R be a function field of one variable over an infinite field k. Then the set of positive integers*

$$G_R = \{[R: k(x)] \mid x \in R,\ x \text{ transcendental over } k\}$$

* Both authors were partially supported by NSF Grants at Purdue University.

0021-8693/82/070062–12$02.00/0

is an additive semigroup, and is defined to be the Lüroth semigroup *of* R *(over* k*).*

Proof. Suppose m and n are in G_R with $m = [R: k(x)]$ and $n = [R: k(y)]$. For a and b in k, we have $(x+a) = (x+a)_0 - (x)_\infty$ and $(y+b) = (y+b)_0 - (y)_\infty$. Since k is infinite, we can choose a, b in k such that $(x+a)_0$ has no prime divisor components in common with $(y)_\infty$, and $(y+b)_0$ has no prime divisor components in common with $(x)_\infty$. For $z = (x+a)(y+b)$, we have $[R: k(z)] = m+n$. Hence G_R is an additive semigroup.

THEOREM 1. *Let* $R \subseteq S$ *be function fields of one variable over an infinite field* k*. Then the Lüroth semigroup of* S, $G_S \subseteq G_R$, *the Lüroth semigroup of* R.

Proof. Let $n \in G_S$, and $x \in S$ be such that $n = [S: k(x)]$. Let y denote the norm of x with respect to the field extension S over R. If y is not algebraic over k, then it follows from [9] that $[S: k(x)] \geqslant [R: k(y)]$. To establish our theorem, it will suffice to show that for some $a \in k$ and $z =$ the norm of $x + a$, we have $[S: k(x)] = [S: k(x+a)] = [R: k(z)]$.

We shall use the notation of [9]. Note that $g_i(x+a) = g_i(x) + a$ in T, and the polar divisor of $g_i(x+a) =$ the polar divisor of $g_i(x)$. Since k is infinite, we can choose $a \in k$ so that the zero divisor of $g_j(x+a)$ has no prime divisor components in common with the polar divisor of $g_i(x+a)$. Hence we have

$$m[T: k(x+a)] = [T: k(z)]$$

and the proof follows verbatim as in [9, p. 86] replacing "$\geqslant$" by "$=$" and "y" by "z."

Remark. If $[S: R] = m$, then we obviously have $mG_R \subseteq G_S$, so that for R and S as in Theorem 1 we have the inclusions $mG_R \subseteq G_S \subseteq G_R$.

It would be interesting to determine if Proposition 1 and Theorem 1 are still valid if the ground field k is finite. Also, for a function field S of n variables over k one may define the *Lüroth set* G_S of S as

$$G_S = \{[S: k(x_1, \ldots, x_n)] \mid x_1, \ldots, x_n \in S \text{ are algebraically independent over } k\}.$$

It would be interesting to know if G_S is always an additive semigroup. Examples such as those in [14, 12, 2] show that for function fields of several variables $R \subseteq S$ one need not have $G_S \subseteq G_R$.

Igusa in [7] generalized the classical Lüroth theorem by proving that if R is a function field of one variable over k such that R is a subfield of a pure transcendental extension in several variables $k(x_1, \ldots, x_n)$, then $R = k(y)$ for

some $y \in R$. If one defines the degree of irrationality, $\operatorname{irr}(S)$, of a function field S of n variables as

$$\operatorname{irr}(S) = \min\{[S: k(x_1,..., x_n)] \mid x_1,..., x_n \in S\}$$

then in analogy with Igusa's theorem, one has

THEOREM 2. *If $R \subseteq S$, with R a function field of one variable, and S a function field of several variables over an infinite ground field k, then the degree of irrationality of S, $\operatorname{irr}(S) \geqslant \operatorname{irr}(R)$, the degree of irrationality of R.*

Proof. Let $m = \operatorname{irr}(S)$ with $m = [S: k(x_1,..., x_n)]$ and $k(x_1,..., x_n)$ pure transcendental over k. If $n = 1$, our result follows from Theorem 1. If $n > 1$, then since R/k has transcendence degree one, we may assume that x_n is transcendental over R. Let $R = k(z_1,..., z_t)$, and let $A = k[x_1,..., x_n, z_1,..., z_t]$. We may assume that A has quotient field S. For $a \in k$ we consider the valuation ring $V = k[x_1,..., x_n]_{(x_n - a)}$. Note that the residue field k_V of the valuation ring V is isomorphic to the field $k(x_1,..., x_{n-1})$, and for all but finitely many $a \in k$, the extensions of V to valuation rings W of the field S are such that $W \supseteq A = k[x_1,..., x_n, z_1,..., z_t]$. Moreover, if $A \subseteq W$, then the center P of W on A is a height one prime of A containing $x_n - a$. Since x_n is transcendental over R, we see that $P \cap k[z_1,..., z_t] = (0)$. Hence, under the canonical map of W to its residue field k_W, we have that R is mapped k-isomorphically on to a subfield of k_W. By a standard result on extending valuation rings [15, p. 285], we have that $[k_W: k_V] \leqslant [S: k(x_1,..., x_n)] = m$. Since $k_V \simeq k(x_1,..., x_{n-1})$, we are reduced now to a situation where $R \subseteq k_W$ a function field of $n - 1$ variables over k and $\operatorname{irr}(k_W) \leqslant m$. A simple induction argument completes the proof.

For fields of characteristic zero we can improve Theorem 2 in a manner similar to the way that Theorem 1 extends our previous result in [9].

THEOREM 3. *If $R \subseteq S$, with R a function field of one variable, and S a function field of several variables over a ground field k of characteristic zero such that k is maximally algebraic in S then the Lüroth set for S, $G_S \subseteq G_R$, the Lüroth semigroup for R.*

Proof. We proceed by induction on the transcendence degree of S over k. If $n = 1$, then the result follows from Theorem 1. Suppose $n > 1$, and let $m \in G_S$ with $m = [S: k(x_1,..., x_n)]$. As in the proof of Theorem 2, we want to obtain a valuation ring $V = k[x_1,..., x_n]_{(f)}$, where f is a linear polynomial in $x_1,..., x_n$, and an extension W of V to S such that the residue field k_W of W contains a k-isomorphic copy of R. Moreover, we now want the equality $[k_W: k_V] = m$. This will follow provided W is unramified over V and is the unique extension of V to S. By [13, p. 68, Lemma 5], for all but finitely

many $b \in k$, $k(x_n - bx_1)$ is maximally algebraic in S. And by "the theorem of Bertini for pencils" [13, p. 61] for all but finitely many $a \in k$ the valuation ring $V = k[x_1, \ldots, x_n]_{(x_n - bx_1 - a)}$ has a unique extension W to a valuation ring of S. Since the valuation ring V is unramified in S for all but at most a finite number of choices of a, we obtain V and W such that $m = [k_W : k_V]$ and, as in the proof of Theorem 2, k_W contains a k-isomorphic copy of R. Thus, for $S' = k_W$, we have $m \in G_{S'}$, and by induction $G_{S'} \subseteq G_R$, so that $m \in G_R$. This completes the proof of Theorem 3.

We conclude this section with a result concerning the structure of the Lüroth semigroup G_R of a function field R of one variable over an algebraically closed ground field k. We shall use the Riemann–Roch formula for divisors D on R [3, p. 210] or [5, p. 295]

$$l(D) = \deg D + 1 - g + l(K - D),$$

where K is any canonical divisor on R, g is the genus of R, and $l(D)$ denotes the vector space dimension of the linear series $\mathscr{L}(D) = \{x \in R \mid (x) + D \geqslant 0\}$.

PROPOSITION 2. *Let R be a function field of one variable of genus g over an algebraically closed ground field k of characteristic zero. Then G_R contains all integers $\geqslant g + 1$.*

Proof. The result is evident for $g = 0$. If $g = 1$, then $K = 0$ is a canonical divisor, and for any prime divisor P the Riemann–Roch formula yields

$$l(P) = \deg P + 1 - 1 = 1.$$

Similarly, we have $l(2P) = 2$ and $l(3P) = 3$. For $x \in \mathscr{L}(2P) \backslash \mathscr{L}(P)$ and $y \in \mathscr{L}(3P) \backslash \mathscr{L}(2P)$, it is clear that $2 = [R : k(x)]$ and $3 = [R : k(y)]$, which settles the case $g = 1$.

For $g > 1$, it follows from the existence of non-Weierstrass points [3, p. 215], that $g + 1, \ldots, 2g - 1 \in G_R$. Moreover, for any prime divisor P, the Riemann–Roch formula implies that $l((n+1)P) = l(nP) + 1$ for all $n > 2g - 2$, since $l(K - nP) = 0$. For any $z \in \mathscr{L}((n+1)P) \backslash \mathscr{L}(nP)$, we have $n + 1 = [R : k(z)]$, which completes the proof of Proposition 2.

Remark. Without assuming that k is of characteristic zero in Proposition 2, we still have for all $n > 2g - 2$ that $l((n+1)P) = l(nP) + 1$, so that G_R contains all integers $\geqslant 2g$.

For k algebraically closed, the semigroup G_R also has the following property: Suppose $R = k(x, y)$, with $[R : k(x)] = m$, $[R : k(y)] = n$, and R is separable algebraic over both $k(x)$ and $k(y)$, then $m + n - 2 \in G_R$, and $m + n - 1 \in G_R$.

Proof. Let $f(\bar{X}, \bar{Y})$ be the defining equation for x and y, and C the corresponding curve. We choose $a, b, c, d \in k$ so that $a \neq b$, $c \neq d$, and

(1) the curve C intersects $x = a$, $x = b$, $y = c$, $y = d$ only at simple points of C,

(2) the curve C contains the points (a, d) and (b, c).

It is easy to see that the zero divisor of the function $z = (x-a)(y-c)/(x-b)(y-d)$ is of degree $n+m-2$. Hence $|R: k(z)| = n+m-2$. To show that $n+m-1 \in G_R$ we simply modify condition (2) by requiring that (a, d) be a point of C, but (b, c) not be a point of C.

2. Weierstrass Canonical Divisors

We shall henceforth assume that the ground field k is algebraically closed. Let R be a function field of one variable over k.

Definition 2. Let K be an effective canonical divisor on R, and let G^K denote the additive semigroup generated by $\{n \mid n = |R: k(x)|$ for some $x \in \mathscr{L}(K)\}$. The canonical divisor K is said to be *Weierstrass* if G^K contains a positive integer less than $g =$ the genus of R.

Proposition 3. *If R has genus g and $n \in G_R$ with $n \leqslant g$, then $n \in G^K$ for some effective canonical divisor K of R.*

Proof. Let $x \in R$ be such that $n = |R: k(x)|$, and let $D = (x)_\infty$. By the Riemann–Roch formula, we have for any canonical divisor K^*

$$l(D) = \deg D + 1 - g + l(K^* - D).$$

Since $l(D) > 1$ and $\deg D \leqslant g$, we have $l(K^* - D) > 0$. Hence there exists $f \in \mathscr{L}(K^* - D)$. Thus

$$(f) + K^* - D \geqslant 0$$

or

$$K = (f) + K^* \geqslant D > 0$$

and $x \in \mathscr{L}(K)$.

Remark. It follows from Propositions 2 and 3 that the computation of the Lüroth semigroup G_R is reduced to the computation of G^K for various effective canonical divisors K of R when R is of characteristic zero.

PROPOSITION 4. *Assume that R has genus $g > 1$, and let K be an effective canonical divisor for R. Then G^K contains at least $g-1$ positive integers $\leqslant 2g-2$.*

Proof. The vector space $\mathscr{L}(K) = \{f \in R \mid (f) + K \geqslant 0\}$ is of dimension g. We shall construct inductively $f_1,\ldots,f_g \in \mathscr{L}(K)$ such that

(1) $(f_1)_\infty > (f_2)_\infty > \cdots > (f_g)_\infty$,

(2) $l((f_i)_\infty) = g + 1 - i$, $i = 1, 2,\ldots, g$.

Note that G^K will then contain the positive integers $\deg(f_i)_\infty$, $i = 1,\ldots, g-1$, thus proving our result. We take f_1 to be a general linear combination of the elements in a basis for $\mathscr{L}(K)$. Then for any $f \in \mathscr{L}(K)$, we have $(f_1)_\infty \geqslant (f)_\infty$ so that $\mathscr{L}(K) = \mathscr{L}((f_1)_\infty)$ and $l((f_1)_\infty) = g$. Suppose, inductively, we have defined $f_1,\ldots,f_i$ satisfying (1) and (2) for some $i < g$. Then $l((f_i)_\infty) = g + 1 - i > 1$, so that $\deg(f_i)_\infty > 0$, say $(f_i)_\infty = \sum n_i P_i$, where the P_i are prime divisors and n_1 is positive. Let

$$U = \left\{ f \in \mathscr{L}((f_i)_\infty) \;\middle|\; (f)_\infty = \sum m_i P_i \text{ with } m_1 < n_1 \right\}.$$

Then U is a proper subspace of $\mathscr{L}((f_i)_\infty)$, and $\mathscr{L}((f_i)_\infty)$ equals the vector space spanned by f_i and U. Hence $\dim U = g - i$. We take f_{i+1} to be a general linear combination of the elements in a basis for U. Then $(f_i)_\infty > (f_{i+1})_\infty$, and $U = \mathscr{L}((f_{i+1})_\infty)$ so that $l((f_{i+1})_\infty) = g - i$. This completes the induction step. and hence the proof.

Remark. We note that classically in the theory of Weierstrass points, there are precisely $g-1$ positive nongaps $\leqslant 2g-1$. However, there are sometimes more than $g-1$ positive integers $\leqslant 2g-2$ in G^K as is indicated by Example 1 in Section 3.

PROPOSITION 5. *Let R be hyperelliptic of genus g. Then G^K is generated by 2 for every effective canonical divisor K, and G_R is generated by 2, $g+1$, $g+2$.*

Proof. It follows from Theorem 9 of [1, p. 74] that there exists a unique genus zero subfield $S \subset R$ with $[R:S] = 2$, and S contains all ratios of differentials of the first kind for R. Therefore $x \in \mathscr{L}(K)$ implies $x \in S$, so that $[R: k(x)]$ is even. Hence G^K consists of only even integers. Proposition 4 implies $2 \in G^K$, and by Proposition 3, G_R contains no odd integer $< g+1$. If R/S is separable, let P be a place of R that is unramified over S. By Proposition 3, $l(gP) = 1$. Hence $l((g+1)P) = 2$ and $l((g+2)P) = 3$, so that $g+1$, $g+2 \in G_R$. If R/S is purely inseparable, let $P_1,\ldots, P_{g+2}$ be distinct places of R, and let $D = P_1 + \cdots + P_{g+2}$. Since every place of R is

ramified over S, $l(D-P_i-P_j)=1$ for any $i\neq j$. Hence $l(D-P_i)=2$, and $l(D)=3$. It follows that there exist functions with polar set precisely $D-P_i$ and D, so that $g+1, g+2\in G_R$.

THEOREM 4. *Let R be a function field of one variable of genus $g>2$ over an algebraically closed ground field k of characteristic zero. Then R is hyperelliptic if and only if every effective canonical divisor for R is Weierstrass.*

Proof. If R is hyperelliptic, then Proposition 5 implies that $2\in G^K$ for every effective canonical divisor K. Hence every K is Weierstrass.

Suppose that R is not hyperelliptic. We consider the canonical embedding of R as a curve C of degree $2g-2$ in projective space $\mathbb{P}^{g-1}$. Effective canonical divisors are given as the $2g-2$ points of $H\cap C$ for H any hyperplane in $\mathbb{P}^{g-1}$. We note that such a canonical divisor $K=H\cap C$ is non-Weierstrass precisely when the $2g-2$ points of $H\cap C$ are in general position—i.e., any $g-1$ of the points span H. This is clear since $f\in\mathscr{L}(K)$ implies $(f)=K^*-K$, where K^* is another effective canonical divisor, say $K^*=H^*\cap C$ with H^* a hyperplane, and $\deg(f)_\infty=2g-2$—(the number of common points of K and K^*). That there exist $K=H\cap C$ for which the points of K are in general position is the content of the following lemma which completes the proof of Theorem 4.

LEMMA (cf. [4, p. 249]). *Let k be an algebraically closed field of characteristic zero, and let C be a curve in projective space $\mathbb{P}^n$, $n>2$, over k such that C is not in any proper linear subspace of $\mathbb{P}^n$. Then there is a hyperplane H in $\mathbb{P}^n$ with the property that any n points of $H\cap C$* span *H.*

Proof. Let B^i denote the set of multi-i-secants for C, $1\leqslant i\leqslant n-2$, that is, $B^i=\{i\text{-dimensional linear subspaces } L \text{ of } \mathbb{P}^n \mid L\cap C \text{ contains more than } i+1 \text{ points}\}$. We claim that B^i is contained in an i-dimensional subset of the set of all i-dimensional planes in $\mathbb{P}^n$.

We first observe that through almost all (i.e., all but at most finitely many) points of C there are only a finite number of multisecant lines. To show this, we just need to show that there exists a point Q of C such that the projection of C with center Q is birational. Since the ground field k is of characteristic zero, the existence of such a point Q on C follows as in [5, p. 311, Proposition 3.8], and the existence of birational projections of C into $\mathbb{P}^3$ (the assumption that the curve is nonsingular is not necessary in [5, Proposition 3.8], one may just consider tangent lines at nonsingular points of the curve). Therefore, the set of multisecant lines (Q_1, Q_2) with Q_1 varying on C but excluding the finite set of points of C having infinitely many multisecants is a 1-dimensional family. For the finitely many exceptional

points Q_1 of C, the set of multisecant lines (Q_1, Q_2) is also 1-dimensional. Hence B^1 is 1-dimensional.

Inductively, we shall assume that B^i is i-dimensional for all $i < j$, where $1 < j \leqslant n-2$. With each multi-j-secant we can associate a $j+2$-tuple $(Q_1,..., Q_{j+2})$ of points of C. If the points $Q_1,..., Q_{j+1}$ are not independent, then they determine a multi-$(j-1)$-secant. By our induction hypothesis, all such multi-j-secants are contained in a j-dimensional family. We therefore consider multi-j-secants associated with $j+2$-tuples $(Q_1,..., Q_{j+2})$ for which $Q_1,..., Q_{j+1}$ are linearly independent. Thus, $(Q_1,..., Q_j)$ span a $(j-1)$-dimensional linear space. We project $\mathbb{P}^n$ to $\mathbb{P}^{n-j}$ using this linear space as the center of our projection. We claim that for almost all $(Q_1,..., Q_j)$—i.e., for all but a $(j-1)$-dimensional subset, such a projection is birational for C. This follows from the fact that C and its projections to $\mathbb{P}^s$, $n > s > n-j$, have the property that through all but a finite number of points there are only a finite number of multisecant lines. The projection with center the linear space spanned by $(Q_1,..., Q_j)$ can be realized by first projecting from Q_1 to $\mathbb{P}^{n-1}$, and then projecting from the image of Q_2 to $\mathbb{P}^{n-2}$ etc. If $(Q_1,..., Q_j)$ is a birational center for C (i.e., the projection of $\mathbb{P}^n$ to $\mathbb{P}^{n-j}$ with center the linear space spanned by $Q_1,..., Q_j$ is birational for C) then there are only finitely many choices of Q_{j+1}, Q_{j+2} to form a multi-j-secant $(Q_1,..., Q_{j+2})$. Hence the set of all multi-j-secants associated with tuples $(Q_1,..., Q_{j+2})$ for which $(Q_1,..., Q_j)$ is a birational center is contained in a j-dimensional family. Furthermore, the multi-j-secants for which $(Q_1,..., Q_j)$ is not a birational center are such that $(Q_1,..., Q_j)$ is in a $(j-1)$-dimensional family. For any such $(Q_1,..., Q_j)$ the corresponding multi-j-secant is uniquely determined by Q_{j+1} which varies on our curve C. Therefore such multi-j-secants are also contained in a j-dimensional family. Our claim on the dimension of B^j is thus established.

We note that the subset of hyperplanes in $\mathbb{P}^n$ that contain a fixed element of B^i is of dimension $n-i-1$. Since B^i has dimension i, it follows that the family of hyperplanes in $\mathbb{P}^n$ that contain some element of B^i is of dimension $n-1$, for each $i = 1, 2,..., n-2$. Let H be any hyperplane in $\mathbb{P}^n$ not in any one of the above $(n-1)$-dimensional sets. If $Q_1,..., Q_n \in H \cap C$, then $Q_1,..., Q_n$ span H. Q.E.D.

Remark. It follows from a classical result about the existence of special divisors [6, Lecture 31, p. 550; 8] that G_R contains integers $\leqslant (g+3)/2$. We conclude that if $g > 3$, then there exist on R Weierstrass canonical divisors. On the other hand, if R is the function field of a nonsingular plane curve of degree 4, so genus 3, we observe in Example 1 that every canonical divisor on R is non-Weierstrass.

3. Applications and Examples

Example 1. Let R be the function field of a nonsingular projective plane curve C of degree n over an algebraically closed ground field k. Then R has genus $g = (n-1)(n-2)/2$, and effective canonical divisors for R are given as the points of intersection of C in $\mathbb{P}^2$ with curves of degree $n-3$. For small values of n, it is easy to calculate the Lüroth semigroup G_R, and show that in fact all nonsingular plane curves of a fixed degree $n < 10$ have the same Lüroth semigroup. If $\mathbb{Z}_+$ denotes the set of positive integers, we have

$$n = 3, \quad \mathbb{Z}_+ \setminus G_R = \{1\},$$
$$n = 4, \quad \mathbb{Z}_+ \setminus G_R = \{1, 2\},$$
$$n = 5, \quad \mathbb{Z}_+ \setminus G_R = \{1, 2, 3\},$$
$$n = 6, \quad \mathbb{Z}_+ \setminus G_R = \{1, 2, 3, 4, 7\},$$
$$n = 7, \quad \mathbb{Z}_+ \setminus G_R = \{1, 2, 3, 4, 5, 8, 9\},$$
$$n = 8, \quad \mathbb{Z}_+ \setminus G_R = \{1,..., 6, 9, 10, 11\},$$
$$n = 9, \quad \mathbb{Z}_+ \setminus G_R = \{1,..., 7, 10, 11, 12, 13\}.$$

To verify the above data we use Proposition 3. For example, to show, for $n = 6$, that $7 \notin G_R$, it follows from Proposition 3 that we only need to show that it is not possible to have two curves of degree $\leqslant 3$ with 7 residual intersections on C. Since two cubics without common component meet in 9 points and $18 - 9 > 7$, while two conics without common component meet in 4 points, and the set of conics in $\mathbb{P}^2$ is 5-dimensional, we see that $12 - 4 = 8 \in G_R$, but $7 \notin G_R$. For $n = 10$, it is not clear if $21 \in G_R$. In order that $21 \in G_R$ one would have to have two distinct cubics in $\mathbb{P}^2$ with 9 common points on C, or two distinct curves of degree 7 meeting in 49 points on C. It is not clear to us if every nonsingular plane curve of degree 10 has such points. In general, it is not hard to show that a canonical divisor K cut out on C by a reducible curve of degree $n-3$ always gives a Weierstrass canonical divisor. We just need to show for m with $1 \leqslant m < n-3$ that

$$mn - (\text{the dimension of curves of degree } m \text{ in } \mathbb{P}^2) + 1 < g.$$

Here $g = (n-1)(n-2)/2$, and $m(m+3)/2$ is the dimension of the family of curves of degree m in $\mathbb{P}^2$, so we wish to show that

$$mn - m(m+3)/2 + 1 < (n-1)(n-2)/2$$

or

$$2mn - m^2 - 3m < n^2 - 3n$$

or

$$0 < (n-m)^2 - 3(n-m) = (n-m)(n-m-3),$$

both of which are positive.

To obtain a canonical divisor K such that G^K contains more than $g-$ positive integers $\leqslant 2g-2$, we consider a nonsingular plane curve C of degr 5, so that $g=6$. Let K be a canonical divisor cut out on C by two lines th do not meet on C. By taking other canonical divisors given by conics wi one of these lines as a component, we see that $4, 5 \in G^K$, and by using tl fact that the family of all conics in $\mathbb{P}^2$ is 5-dimensional, we obtain oth conics that cut out any number between 0 and 4 points of K. Thus, 6, 7, $9, 10 \in G^K$, and G^K contains $g+1$ positive integers $\leqslant 2g-2$.

We note that the above data on Lüroth semigroups together wi Theorem 1 yields some information on the impossibility of $R \subseteq S$, for R ar S function fields of nonsingular plane curves. For example, if R and S a function fields of nonsingular plane curves of degree 6 and 8, respectivel then $7 \in G_S \backslash G_R$ implies $R \not\subseteq S$. This is a case not ruled out by Hurwitz theorem relating the genera of R and S when $R \subseteq S$. For a classic treatment of Proposition 6, see J. L. Coolidge, *A Treatise on Algebraic Pla Curves*, p. 408.

PROPOSITION 6. *Let R and S be function fields of nonsingular projecti plane curves C and C^* of the same degree $n \geqslant 4$ over an algebraically clos ground field k. Then any k-isomorphism $\tau: R \to S$ is induced by a line isomorphism $\sigma: \mathbb{P}^2 \to \mathbb{P}^2$ such that $\sigma(C) = C^*$.*

Proof. Let $R = k(x, y)$, $S = k(u, v)$ be given by affine pieces of t embeddings of C and C^* into $\mathbb{P}^2$. We just need to show that $\tau(x)$ and $\tau($ are fractional linear in u and v. If $n=4$, then effective canonical divisors a cut out by lines, so that $(x)_0$ and $(x)_\infty$ are canonical divisors for R. Hen $(\tau(x))_0$ and $(\tau(x))_\infty$ are canonical divisors for S, so that $\tau(x)$, and similar $\tau(y)$ are fractional linear in u and v. If $n \geqslant 5$, then $\deg(x)_\infty = \deg(\tau(x))_\infty$ $n <$ genus of $C = (n-1)(n-2)/2$, so it follows from Proposition 3 th $\tau(x) \in \mathscr{L}(K^*)$, for some effective canonical divisor K^* of S. Let K^* be giv as the intersection of C^* with a curve F of degree $n-3$ defined b $f(\bar{U}, \bar{V}) = 0$. Then $\tau(x) + K^*$ is another effective canonical divisor for S, sa cut out by a curve G defined by $g(\bar{U}, \bar{V}) = 0$. We have $\tau(x) = g(u, v)/f(u, v)$ and we need to show that F and G have a common component of degr $n-4$. Suppose $F = F^* \cup E$, $G = G^* \cup E$ with F^* and G^* having r common components and $\deg E = n-3-i$, $1 \leqslant i \leqslant n-3$. so that $\deg F^*$ $\deg G^* = i$. We have

$$\#(F^* \cap C^*) = \#(G^* \cap C^*) = in$$

and

$$\#(F^* \cap G^*) = i^2.$$

Since $\deg(\tau(x))_0 = \deg(\tau(x))_\infty \leqslant n$, we have

$$\#(F^* \cap C^*) \leqslant \deg(\tau(x))_\infty + \#(F^* \cap G^*) \leqslant n + i^2.$$

Thus,

$$in \leqslant n + i^2,$$

or

$$i(n-i) - n = (i-1)(n-i-1) - 1 \leqslant 0,$$

which implies $i = 1$. Q.E.D.

Remark. Proposition 6 is not true for nonsingular plane curves of degree 3. For example, if k is of characteristic zero, and $R = k(x, y)$, with $y^2 - 2x^2y + x = 0$, then consider the following change of variables: let $y_1 = y - x^2$ so that $y_1^2 + x - x^4 = 0$. Let $u = y_1/x^2$ and $v = 1/x$ so that $u^2 + v^3 - 1 = 0$, and $R = k(x, y) = k(u, v) = S$. The 3 points $u = 0$, $y = 1$, w, w^2, where w is a primitive 3rd root of unity are collinear for $k(u, v)$, but lie on the irreducible conic $y = x^2$ for $k(x, y)$.

EXAMPLE 2. Let S be a function field of one variable over an algebraically closed ground field k. If S is a trigonal field, i.e., $3 \in G_S$, then any hyperelliptic subfield R of S is of genus 2.

Proof. Since $3 \in G_S \subseteq G_R$, we have $2, 3 \in G_R$. Let $x, y \in R$ be such that $[R: k(x)] = 2$ and $[R: k(y)] = 3$. Then $R = k(x, y)$. Let $f(\bar{X}, \bar{Y}) = 0$ be the defining equation of x, y. Then

$$\deg_{\bar{Y}} f(\bar{X}, \bar{Y}) = 2 \qquad \text{and} \qquad \deg_{\bar{X}} f(\bar{X}, \bar{Y}) = 3.$$

If the total degree of $f(\bar{X}, \bar{Y}) = 3$, then R is of genus $\leqslant 1$ contrary to our assumption that R is hyperelliptic. Hence $f(\bar{X}, \bar{Y})$ has degree 4 or 5. Moreover, from Example 1, we see that $f(\bar{X}, \bar{Y})$ must define a singular projective plane curve. If $f(\bar{X}, \bar{Y})$ is of degree 4, then the genus of R is $\leqslant 2$ [3, p. 201], as we wish to show. If $f(\bar{X}, \bar{Y})$ is of degree 5, then by a linear change of variables, we may assume that $f(0, 0) = 0$. Consider

$$(1/\bar{X}^3\bar{Y}^2) \cdot f(\bar{X}, \bar{Y}) = g(1/\bar{X}, 1/\bar{Y}).$$

It is easy to see that $g(1/\bar{X}, 1/\bar{Y})$ has degree at most 4. Hence, as above, we conclude that R is of genus $\leqslant 2$.

REFERENCES

1. C. CHEVALLEY, "Introduction to the Theory of Algebraic Functions of One Variable," Amer. Math. Soc., New York, 1951.
2. C. CLEMENS AND P. GRIFFITHS, The intermediate Jacobian of the cubic threefold, *Ann. of Math.* **95** (1972), 281–356.
3. W. FULTON, "Algebraic Curves," Benjamin, New York, 1969.
4. P. GRIFFITHS AND J. HARRIS, "Principles of Algebraic Geometry," Wiley, New York, 1978.
5. R. HARTSHORNE, "Algebraic Geometry," Springer-Verlag, New York, 1977.
6. K. HENSEL AND G. LANDSBERG, "Theorie der Algebraischen Funktionen Einer Variabeln," Chelsea, New York, 1965.
7. J. IGUSA, On a theorem of Lüroth, *Mem. Univ. Kyoto* **26** (1950–1951), 251–253.
8. S. KLEIMAN AND D. LAKSOV, Another proof of the existence of special divisors, *Acta Math.* **132** (1974), 163–176.
9. T. T. MOH AND W. HEINZER, A generalized Lüroth theorem for curves, *J. Math. Soc. Japan* **31** (1979), 85–86.
10. M. NAGATA, A theorem on valuation rings and its application, *Nagoya Math. J.* **29** (1967), 85–91.
11. P. SAMUEL, Some remarks on Lüroth's theorem, *Mem. Univ. Kyoto* **27** (1953), 223–224.
12. R. SWAN, Invariant rational functions and a problem of Steenrod, *Invent. Math.* **7** (1969), 148–158.
13. O. ZARISKI, Pencils on an algebraic variety and a new proof of a theorem of Bertini, *Trans. Amer. Math. Soc.* **50** (1941), 48–70.
14. O. ZARISKI, On Castelnuovo's criterion of rationality, $p_a = P_2 = 0$ of an algebraic surface, *Illinois J. Math.* **2** (1958), 303–315.
15. O. ZARISKI AND P. SAMUEL, "Commutative Algebra," Vol. I, Van Nostrand, Princeton, N.J., 1958.